Appl. No. 09/622,047
Reply to Office Action of January 18, 2006

Attorney Docket: P65855US0

Amendments to the Claims:

The listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method for block encryption of discrete data, comprising the steps of: generating an encryption key in the form of a set of subkeys, breaking down a data block into $N \geq 2$ data subblocks and alternately converting said data subblocks by performing a two-place operation on the data subblock and the subkey, wherein, prior to carrying out said two-place operation on an i-th data subblock and a subkey, an operation of permuting subkey bits a substitution operation is performed on the subkey depending on the value of a j-th data subblock, where $i \neq j$.

Claim 2 (cancelled)

Claim 3 (currently amended): The method according to claim 12, wherein an operation of cyclic offsetting subkey bits depending on the value of the j-th data subblock is used as the j-th data subblock-dependent operation of permuting subkey bits.

Claim 4 (cancelled)

Claim 5 (new) The method according to claim 1, wherein the operation of permuting subkey bits is performed on one of said set of subkeys depending on the value of the j-th data subblock, where $i \neq j$, and the value of another subkey.